

**ENHANCING DECEPTION IN REALISTIC HTTP HONEYPOTS TO
STIMULATE AND REVEAL ATTACKER BEHAVIOR THROUGH ATTACK
SESSION-BASED ANALYSIS**

By

Andi Parada Tambunan

22451013

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

August 2025

**ENHANCING DECEPTION IN REALISTIC HTTP HONEYPOTS TO
STIMULATE AND REVEAL ATTACKER BEHAVIOR THROUGH ATTACK
SESSION-BASED ANALYSIS**

By

Andi Parada Tambunan

22451013

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

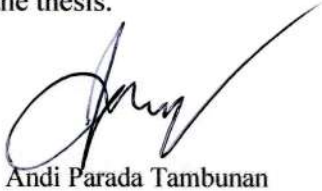


SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

August 2025

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.



Andi Parada Tambunan

Student

24 August 2025

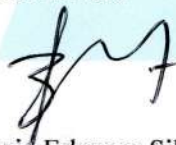
Approved by:



Dr. Ir. Charles Lim BSc., MSc.

Thesis Advisor

24 August 2025



Kalpin Erlangga Silaen, S.Si., M.Kom.

Thesis Co-Advisor

24 August 2025

Dr. Maulahikmah Galinium, S.Kom., M.Sc.

Dean of Faculty of Engineering and
Information Technology

24 August 2025

Andi Parada Tambunan

ABSTRACT

ENHANCING DECEPTION IN REALISTIC HTTP HONEYPOTS TO STIMULATE AND REVEAL ATTACKER BEHAVIOR THROUGH ATTACK SESSION-BASED ANALYSIS

By

Andi Parada Tambunan

Dr. Ir. Charles Lim BSc., MSc. , Advisor

Kalpin Erlangga Silaen, S.Si., M.Kom., Co-Advisor

SWISS GERMAN UNIVERSITY

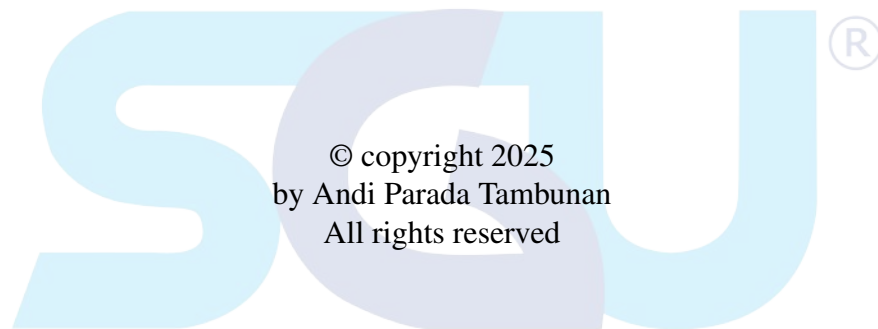


The digital transformation era has dramatically increased the global dependency on web services, consequently elevating the risks associated with cybersecurity threats. As the integration of digital technologies into business operations becomes more prevalent, the sophistication of cyber threats continues to evolve, targeting vulnerabilities across various digital platforms. This research aims to address these escalating security challenges by enhancing the deceptive capabilities of honeypots, thereby improving the detection and analysis of sophisticated cyberattacks. Specifically, this study integrates vulnerabilities listed in the OWASP Top 10 2021 and employs the MITRE ATT&CK framework to develop a honeypot that not only simulates real-world systems but also provides a structured analysis of attacker tactics, techniques, and procedures (TTPs). This approach promises to increase the engagement of attackers with honeypots, thereby enriching the data available for enhancing cybersecurity measures. The literature review reveals a significant reliance on honeypots to capture and analyze advanced threats, highlighting their evolving role in the cybersecurity landscape. This study contributes to the field by proposing a refined honeypot model that leverages established security frameworks to offer more realistic interactions and comprehensive

threat analyses. The expected outcome is to provide deeper insights into cyber attacker behaviors, thus supporting the development of more effective cybersecurity strategies to protect against a broader spectrum of cyber threats.

Keywords: Cybersecurity, Honeypots, HTTP, OWASP Top 10, MITRE ATT&CK





© copyright 2025
by Andi Parada Tambunan
All rights reserved

DEDICATION

This work is dedicated to the progress of honeypot technology in Indonesia



ACKNOWLEDGEMENT

The author gratefully acknowledges the Thesis Advisor and Thesis Co-Advisor for their scholarly guidance, constructive feedback, and exemplary mentorship throughout this research. Their support refined the theoretical framing, strengthened methodological rigor, and deepened the author's understanding of the design and practical application of honeypots.

Appreciation is also extended to the research assistant team for their contributions to data collection, preprocessing, and validation, as well as for discussions that sharpened the analysis. This collaboration contributed materially to the quality of the findings and the completion of the manuscript.

The author further thanks family and partner for sustained moral and material support, and all individuals and institutions that provided assistance in various forms. These contributions constituted an essential foundation for the completion of this thesis and for the author's continued academic and professional development.

Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	5
ACKNOWLEDGEMENT	6
TABLE OF CONTENTS	9
LIST OF FIGURES	10
LIST OF TABLES	11
LIST OF PUBLICATIONS	12
1. INTRODUCTION	14
1.1 Background	14
1.2 Problem Statement	16
1.3 Research Objective	16
1.4 Research Question	18
1.5 Significance of Study	18
1.6 Hypothesis	19
1.7 Scope of the Problem	19
1.7.1 Realistic HTTP Honeypot Development	19
1.7.2 Attacker Behavior Analysis	19
1.8 Research Roadmap	20
1.9 Thesis Structure	21

2. LITERATURE REVIEW	22
2.1 HTTP Protocol	22
2.1.1 HTTP: History and Evolution	22
2.1.2 HTTP Vulnerabilities	23
2.2 The Impact of Digital Business Transformation on Cybersecurity	24
2.2.1 Cybersecurity Challenges in Web-based Services	25
2.2.2 Deception-based Solutions in Cybersecurity	26
2.2.3 The Role of HTTP Honeypots in Attack Detection and Deception	27
2.3 Honeypot Capabilities	28
2.3.1 Fundamentals of Honeypots	28
2.3.2 Capabilities and Challenges of Honeypots	29
2.3.3 Enhancing Honeypot Realism for Cyber Deception	30
2.4 Understanding Attacker Behavior	31
2.4.1 Tactics, Techniques, and Procedures (TTPs) in Attacker Behavior Analysis	32
2.4.2 Limitation of Single Event Analysis	32
2.4.3 Attack Session-Based Analysis	33
2.4.4 Machine Learning	34
2.5 Our Research Journey	35
2.6 Related Works	38
3. RESEARCH METHODS	44
3.1 Overview	44
3.2 Research Framework	44
3.3 Development and Deployment	45
3.4 Data Collection	45
3.5 Analysis	46
3.6 Evaluation	46
4. EXPERIMENT AND RESULTS	49
4.1 System Implementation Overview	49
4.1.1 Hardware Environment	49
4.1.2 Software Setup	50

4.1.3	Configuration Parameters	52
4.2	Data Collection	52
4.3	Analysis	53
4.3.1	Machine Learning Setup	55
4.4	Evaluation	56
4.4.1	Engagement Duration	56
4.4.2	Interaction Complexity	57
4.4.3	Deception Success Rate	58
4.5	Validation	60
4.5.1	Engagement Duration	60
4.5.2	Interaction Complexity	62
4.5.3	Deception Success Rate	65
4.6	Summary and Findings	69
5.	CONCLUSIONS AND RECOMMENDATIONS	72
5.1	Conclusion	72
5.2	Future Work	72
	REFERENCES	83
	Appendix 1: Exploitation Activity	84
	Appendix 2: Session Mapping TTPs	93

List of Figures

1.1	Monthly Web Attacks in 2023	15
1.2	Fishbone Diagram	17
1.3	Research Roadmap	20
3.1	Research Framework	44
3.2	Evaluation between Common and Custom Honeypots	47
4.1	Supervised Learning Training Phase Result	54
4.2	Supervised Learning Testing Phase Result	54
4.3	Unsupervised Learning Result	55
4.4	Top IP Attacker in Custom Honeypot	58
4.5	Custom Honeypot Anti-Detection Shodan Check	59
4.6	Top IP Attacker in Custom Honeypot	63
4.7	Top IP Attacker in Hellpot	63
4.8	Top IP Attacker in Express Honeypot	64
4.9	Top IP Attacker in Honeytrap	64
4.10	Top IP Attacker in OpenCanary	64
4.11	Custom Honeypot Anti-Detection Shodan Check	67
4.12	Hellpot Anti-Detection Shodan Check	67
4.13	OpenCanary Anti-Detection Shodan Check	67
4.14	Honeytrap Anti-Detection Shodan Check	68
4.15	Express Honeypot Anti-Detection Shodan Check	68

List of Tables

2.1	Honeypot Capability Metrics	31
2.2	Related Works	43
4.1	Hardware Used	50
4.2	Summary of Key Honeypot Log Attributes	52
4.3	Session-Based Average Dwell Time (Custom Honeypot)	56
4.4	Request Statistics per Session (Custom Honeypot)	57
4.5	Exploit Attempts (Custom Honeypot)	57
4.6	Session Mapping to MITRE ATT&CK (Custom Honeypot)	57
4.7	Interaction Type Breakdown (Custom Honeypot)	58
4.8	URI and Payload Diversity (Custom Honeypot)	58
4.9	Follow-up Response Analysis (Custom Honeypot)	59
4.10	Anti-Detection Resistance (Custom Honeypot)	59
4.11	Evade Rate (Custom Honeypot)	60
4.12	Ratio of Human/Tool to Automated Sessions (Custom Honeypot)	60
4.13	Session-Based Average Dwell Time per Honeypot	61
4.14	Request Statistics per Session	61
4.15	Statistic Exploitation Per Honeypot	61
4.16	Session Mapping To MITRE ATT&CK	62
4.17	Interaction Type Breakdown	65
4.18	URI and Payload Diversity	65
4.19	Follow-up Response Analysis	66
4.20	Anti-Detection Resistance: Percentage of IPs with Only One Session (Lower is Better)	68
4.21	Evade Rate: Premature Session Termination	69
4.22	Ratio of Human/Tool to Automated Sessions	69

List of Publications

This chapter provides a record of the research contributions made throughout the academic journey. The listed publication highlights the work conducted in the domain of cybersecurity, focusing on honeypot enhancements and attacker profiling.

1. Attack Session-Based Analysis to Reveal HTTP Attacker Behavior

Status: Accepted

Acceptance Date: March 3rd, 2025

Presentation Date : April 4-6th, 2025

Publisher: Springer Lecture Notes in Networks and Systems Series

Summary: This paper applies Attack Session-Based Analysis to enhance HTTP attack detection by correlating multiple attacker actions within a session, addressing the limitations of single-event analysis. Using a custom HTTP honeypot, it analyzes 147,079 attack events to map structured attack sequences to MITRE ATT&CK, reducing misclassification and false positives through Idle Time-Based and Variable-Based Session Identification. The approach improves cyber threat intelligence, with future directions exploring machine learning and graph-based clustering for advanced attacker profiling

2. Bot, Tool, or Human? A Machine Learning Approach to Web Attacker Behavior Analysis

Status: Under Review

Submission Date: August 23rd, 2025

Presentation Date: Pending (Expected per conference timeline: September 8th, 2025, Extend III)

Conference: International Conference on Computational Intelligence and Cybersecurity (ICoCIC 2025)

Publisher: IEEE

Summary: This paper introduces a multi-stage machine learning framework to classify HTTP-based attackers into three categories: bots, automation tools, and humans. Using over 185,000 honeypot log entries, the approach combines supervised learning (Random Forest and XGBoost) with unsupervised clustering (K-Means) to separate automated and semi-automated behaviors from human-driven attacks. The framework enhances attacker profiling by revealing nuanced adversarial behaviors, moving beyond the traditional bot versus human dichotomy, and contributes to more adaptive threat detection and intelligence.

